Attorney's Docket No.: 1999P7519US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : George E. Carter
Serial No. : 09/277,298
Filed : March 26, 1999
Title : METHODS AND APPARATUS FOR KERNEL MODE ENCRYPTION OF COMPUTER TELEPHONY

Art Unit : 2131
Examiner : Arani, Taghi T.

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO THE EXAMINER'S ACTION DATED JULY 23, 2004

Certificate of Facsimile Transmission

I hereby certify that this document is being facsimile transmitted on the below listed date, consisting of the below listed number of pages, and to the below listed fax number.

Date of Trans.: October 15, 2004
Fax Number: 703-872-9306
No. of Pages: Nine (9) Total
By: Jeanette L. Taplin

I. Status of claims

There are no amendments to the claims.

Claims 1-11, 13, 14, and 16-35 are pending.

Claims 13, 14, and 16-31 have been allowed.

II. Rejection of claims 1-11 and 32-35

A. Claims 1, 8, and 32-35

The Examiner has rejected claims 1, 8, and 32-35 under 35 U.S.C. § 103(a) over Knappe (U.S. 6,603,774) in view of Solomon (U.S. 5,974,043).

Independent claims 1 and 8 recite that a security algorithm is inserted within the communication path between the first telephony client on the first computer and a sound device on the first computer, with the security algorithm performing cryptographic operations on audio data transmitted in at least one direction between the first telephony client and the sound device.

The Examiner has relied on the teaching of Solomon to make up for Knappe's failure to teach or suggest anything about inserting a security algorithm within a communication path between telephony clients. In particular, the Examiner has asserted that:

> Solomon further discloses inserting a security algorithm within the communication path between first telephony client and a sound device on the first computer, the security algorithm performing cryptographic operations (i.e., encrypting and decrypting) on audio data transmitted in at least one direction between the first telephony client and the sound device, see col. 4, line 61 through

col. 5, line 34, see also col. 8, lines 19-36, col. 14, lines 39-61, col. 19, lines 31-42, col. 23, lines 39-52.

As the following detailed analysis of Solomon's disclosure reveals, however, Solomon merely indicates that computers 4 may be configured to encrypt/decrypt telephony signals that are exchanged between the computers 4. Solomon does not provide any details about how the computers 4 encrypt/decrypt the telephony signals. Therefore, contrary to the Examiner's assertion, Solomon does not disclose inserting a security algorithm within the communication path between first telephony client and a sound device on the first computer. For this reason, the Examiner has failed to establish a proper *prima facie* rejection of claims 1 and 8 under 35 U.S.C. § 103 in which "the prior art reference (or references when combined) must teach or suggest all the claim limitations" (MPEP § 706.02(j)).

Location in Solomon's Disclosure (col./line numbers)	Quoted Text of Solomon's Disclosure	Analysis
4/61-64	Additionally, in accordance with yet another preferred embodiment of the present invention, the step of exchanging further includes the step of encrypting the information before exchanging it.	Merely teaches that telephony signals are encrypted before being exchanged. There is no teaching that a security algorithm is inserted within the communication path between the first telephony client and a sound device on the first computer.
4/65 – 5/2	In accordance with another preferred embodiment of the present invention, the data block of the step of sending further includes a public key for decrypting encrypted information which was generated by the step of encrypting and exchanged by the step of exchanging.	Merely teaches that the encrypted data block includes a public key. There is no teaching that a security algorithm is inserted within the communication path between the first telephony client and a sound device on the first computer.

5/3-24	Further, in accordance with an additional preferred embodiment of the present invention, the information which is exchanged in the step of exchanging is voice information or control information or data files or graphic information or video information or any combination thereof. Additionally, in accordance with an additional preferred embodiment of the present invention, the information which is exchanged in the step of exchanging is analog information or digital information or a combination of analog information and digital information. Still further, in accordance with another preferred embodiment of the present invention, the step of exchanging is selected from the group of steps consisting of: the step of transferring the information unidirectionally from the first communication system to the second communication system, the step of transferring the information unidirectionally from the second communication system to the first communication system and the step of bidirectionally transferring the information from the first communication system to the second communication system and from the second communication system to the first communication system.	There is no teaching that a security algorithm is inserted within the communication path between the first telephony client and a sound device on the first computer.
5/25-34	Yet, according to an additional preferred embodiment of the present invention, at least one of the first communication system and the second communication system also includes at least one device for processing information which is connected to the computer. The device for processing information is a videophone device or a video-conferencing device or a sound card connected to a microphone and earphones or a sound card connected to a microphone and a speaker. The device for processing information inputs or outputs the exchanged information.	Merely teaches that at least one of the first and second communication systems may include a sound card. There is no teaching that a security algorithm is inserted within the communication path between the first telephony client and a sound device on the first computer.
8/19-36	It is further noted that a feature of the present invention is the ability of the computers 4 to scramble and descramble the digital data transferred between the modems in the modem or WAN modes. This has the advantage that the	Merely teaches that the computers 4 can scramble and descramble the digital data transferred between the modems. There is no

	users can conduct a high security, scrambled, voice telephone conversation in the modem mode, thus protecting the conversation from interception and wiretapping. The high security scrambling of data transmission can also be used when the WAN telephone system 6 is used for initiating the transfer of other types of digital data such as a facsimile transmission between the computers 4 in the modem or WAN modes. Thus, the user of the WAN telephone system 6 enjoys the advantages of high security scrambled voice and data transmission by using the processing power of an existing computer, without having to purchase an expensive scrambling telephone instrument or expensive scrambling equipment.	teaching that a security algorithm is inserted within the communication path between the first telephony client and a sound device on the first computer.
14-39-61	The fast format data block can also include additional information containing caller identification data such as the caller's name or the caller's telephone number or the caller's E-mail address or any other caller related data for supplying the destination user with information about the caller. The fast format data block can also include a Public Key data which may be required for data encryption in the direct scrambled call or for data encryption in the WAN call. It is noted that the scrambling or the encryption methods used by the WAN telephone system can be any suitable scrambling or encryption methods. It is also noted that the fast format data block can include more than one Public Key for encryption. The system then checks whether a fast format acknowledge (ACK) signal is received the destination telephone (step 216). If the system does not receive a fast format ACK signal within a predetermined time interval or if the system receives a fast format negative acknowledge (NACK) signal, the system interprets this as an indication that the destination telephone is unable to perform descrambling and alerts the user that a scrambled call cannot be accomplished (step 218) the user then may conduct an unscrambled telephone conversation (step 206).	Merely teaches that the fast format data block can include a Public Key data. There is no teaching that a security algorithm is inserted within the communication path between the first telephony client and a sound device on the first computer.

19/31-42	The exchanged information can be any type of digital information such as compressed or non-compressed voice information, compressed or noncompressed video information or data files containing any other type of digital information. The information can also be encrypted and decrypted by the computers 355 using any suitable data encryption and decryption method (not shown). After the information is exchanged between the WAN telephone systems, the system disconnects from the WAN (step 450) and transfers control to step 420.	Merely teaches that the computers 355 can encrypt and decrypt the exchanged information. There is no teaching that a security algorithm is inserted within the communication path between the first telephony client and a sound device on the first computer.
23/39-45	9. A telephone according to claim 1 and wherein said computer also comprises a sound card for digitizing analog voice signals of said user received from said at least one communication unit and for converting digital voice data received by said computer from said WAN into analog voice signals, said analog voice signals being communicated through said controller to said at least one communication unit.	Merely teaches that the computer includes a sound card. There is no teaching that a security algorithm is inserted within the communication path between the first telephony client and a sound device on the first computer.
23/46-49	10. A telephone according to claim 1 and wherein said information is encrypted by said computer prior to being communicated through the PSTN.	Merely teaches that the computer encrypts the information before the information is communicated through the PSTN. There is no teaching that a security algorithm is inserted within the communication path between the first telephony client and a sound device on the first computer.
23/50-52	11. A telephone according to claim 1 and wherein said information is decrypted by said computer after being received through the PSTN.	Merely teaches that the computer decrypts the information after the information is received through the PSTN. There is no teaching that a security algorithm is inserted within the communication path between the first

		telephony client and a sound device on the first computer.

As revealed by the detailed analysis provided above, the Examiner cannot reasonably maintain his position that Solomon teaches that a security algorithm is inserted within the communication path between the first telephony client on the first computer and a sound device on the first computer, as recited in claims 1 and 8. Indeed, Solomon fails to provide any hint about where his encryption/decryption algorithm could be placed in the computers 4. The only reference cited by the Examiner that teaches anything about where a security algorithm should be placed is Kavsan. Kavsan, however, teaches that security for the outgoing and incoming communications of a computer is provided by placing a security enabled engine 14 between an application program 12 and an internet port 26. Therefore, based on the art cited by the Examiner, one of ordinary skill in the art would have been led to place a security enabled engine 14 between telephony applications and the modems in Solomon's computers 4. One of ordinary skill in the art would have been led away from the invention of claims 1 and 8 in which a security algorithm is inserted within the communication path between the first telephony client on the first computer and a sound device on the first computer because he/she reasonably would have concluded that the security enabled engine 14 positioned between the telephony application and the modem would have been sufficient to protect incoming/outgoing communications.

Thus, the Examiner has failed to establish a proper *prima facie* case of obviousness under 35 U.S.C. § 103(a) because the combination of Knappe and Solomon does not teach or suggest all the claim elements recited in claims 1 and 8. Moreover, the combination of the disclosures of all of the art cited by the Examiner teaches away from the invention recited in claims 1 and 8.

For at least these reasons, the Examiner's rejection of independent claims 1 and 8 under 35 U.S.C. § 103(a) over Knappe in view of Solomon should be withdrawn.

Claims 32 and 33 incorporate the features of independent claim 1 and claims 34 and 35 incorporate the features of independent claim 8. Therefore, claims 32-35 are patentable for at least the same reasons explained above.

B. Claims 2, 3, 6, 7, 9, and 10

The Examiner has rejected claims 2, 3, 6, 7, 9, and 10 under 35 U.S.C. § 103(a) over Knappe in view of Solomon and Kavsan (U.S. 6,412,069).

Claims 2, 3, 6, and 7 incorporate the features of independent claim 1 and claims 9 and 10 incorporate the features of independent claim 8. Kavsan does not make-up for the failure of Knappe and Solomon to teach or suggest inserting a security algorithm within the communication path between the first telephony client on the first computer and a sound device on the first computer. Indeed, Kavsan fails to teach or suggest anything about a security algorithm that performs cryptographic operations on audio data transmitted in at least one direction between a first telephony client *and a sound device* on the same computer, as recited in claims 1 and 8. In Kavsan's approach, the security enabled engines 14 are inserted between the associated application programs 12 and an internet port 24, a disk drive 20, and a hard drive 22; none of the security enabled engines 14 is inserted between a telephony client and a sound device on the same computer, as recited in independent claims 1 and 8. Indeed, one of ordinary skill in the art would not have been motivated to provide a security enabled engine between an application program 12 and a sound device because he/she reasonably would have concluded that the security enabled engine 14 positioned between the application program 12 and the internet port 24 would have been sufficient to protect incoming/outgoing communications. Therefore, claims 2, 3, 6, 7, 9, and 10 are patentable for at least the same reasons explained above.

It is noted that the Examiner has copied verbatim from his prior action the incorrect assertion that the "teaching of Kavsan clearly suggests encrypting audio data received from the sound device (at the drive level) and providing the encrypted data to the cryptographic software situated at the application space and decrypting signals received from the application space at the kernel space." Kavsan does not even hint that the security enabled engines 14 could be inserted between the application programs 12 and sound devices on the same computer. The mere fact that Kavsan's approach is implemented at the driver level does not constitute a teaching or suggestion to insert a security enabled engine 14 between an application 12 and a sound device. Indeed, based on Kavsan's teaching one of ordinary skill in the art designing a telephony system would have inserted a security enabled engine 14 between a telephony application 12 and the

internet port 24, as shown in Kavsan's only drawing sheet. It appears that the Examiner improperly has engaged in hindsight reconstruction of the claimed invention using applicant's disclosure as a blueprint for piecing together prior art to defeat patentability.

The Examiner also has incorrectly asserted that:

> It would have been obvious to one of ordinary skill in the art to modify Solomon's invention to employ cryptographic service software of Kavsan in Knappe's method of voice packets in telephony application to provide encryption/decryption to telephony clients to conduct encrypted communication at the driver level of the client computer, because application level cryptographic services CryptoAPI™ would not work at the driver level where IP packets need to be encrypted, see col. 1, lines 47-61.

The Examiner's asserted motivation for combining the teachings of Knappe, Solomon, and Kavsan, however, is not persuasive. Indeed, Knappe fails to teach or suggest anything about incorporating any kind of security algorithm in his approach and Kavsan fails to teach or suggest anything about telephony applications. The mere fact that the CryptoAPI™ software cannot operate in the kernel space would not have motivated one of ordinary skill in the art at the time of the invention to incorporate Kavsan's method in Knappe's proxy transcoding system. Without a proper explanation for combining Knappe and Kavsan, the Examiner has failed to establish a proper *prima facie* case of obviousness and the rejection should be withdrawn.

To summarize, neither Knappe nor Solomon nor Kavsan teaches or suggests anything about inserting a security algorithm within the communication path between the first telephony client on the first computer and a sound device on the first computer, as recited in claims 1 and 8. Accordingly, no permissible combination of Knappe, Solomon, and Kavsan could teach or suggest such a feature.

For at least the reasons explained above, the Examiner's rejection of claims 2, 3, 6, 7, 9, and 10 under 35 U.S.C. § 103(a) over Knappe in view of Solomon and Kavsan should be withdrawn.

C. Claim 11

The Examiner has rejected claim 11 under 35 U.S.C. § 103(a) over Knappe (U.S. 6,603,774) in view of Solomon (U.S. 5,974,043).

Independent claim 11 recites that secure communication between the first and second telephony clients is facilitated by performing cryptographic operations on audio data transmitted in at least one direction between the first telephony client and a sound device on the first computer.

As explained above in connection with independent claims 1 and 8, neither Knappe nor Kavsan teaches or suggests anything about a security algorithm that performs cryptographic operations on audio data transmitted in at least one direction between a first telephony client and a sound device on the same computer.

For at least these reasons, the Examiner's rejection of independent claim 11 under 35 U.S.C. § 103(a) over Knappe in view of Kavsan now should be withdrawn.

IV. Conclusion

For the reasons explained above, all of the pending claims are now in condition for allowance and should be allowed.

Charge any excess fees or apply any credits to Deposit Account No. 19-2179.

Date: 14 Oct 04

Respectfully requested,

By: _____
David D. Chung
Registration No. 38,409
Attorney for Applicants
Tel: 650-694-5339
Fax: 650-968-4517

SIEMENS CORPORATION
Customer Number: 28524
Intellectual Property Department
170 Wood Avenue South
Iselin, New Jersey 08830
ATTENTION: Elsa Keller, IP Department
Telephone: (732) 321-3026